UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 18-CR-157

THOMAS J. OWENS,

Defendant.

ORDER DENYING MOTION TO COMPEL

Defendant Thomas J. Owens has been charged by a Grand Jury with Distribution and Possession of Child Pornography in violation of 18 U.S.C. § 2252A(a)(2) and (5)(B). The charges grew out of an investigation conducted by the Oshkosh Police Department over the BitTorrent Network where individuals are known to share child pornography. In conducting its investigation, Oshkosh police officers used an investigative software program called "Torrential Downpour Receptor" (TDR), which is designed to connect to the BitTorrent Network and identify IP addresses for computers that make available shared folders containing files with hash values known to be associated with child pornography. After TDR detected and downloaded targeted hash values depicting child pornography at an IP address later identified with Owens' residence, a search warrant was executed, during which officers obtained thousands of depictions of child pornography. Notwithstanding the discovery of numerous other depictions of child pornography on Owens' computer, law enforcement was unable to locate the child pornography video that it downloaded from his computer and that forms the basis of the distribution charge against him. Owens argues this is evidence that he never possessed that video and that TDR is defective.

Presently before the court is the defendant's motion to compel the government to disclose to the defense "copies of (or other satisfactory access to) all investigative software programs used in the case, including all supporting documents such as user's manuals, technical specifications and white papers related to any software used." Dkt. No. 19. Owens contends that copies of the investigative software programs used by law enforcement are necessary for him to conduct his defense. More specifically, Owens notes that the child pornography he is alleged to have distributed to the undercover agent was not found on his computer. He suggests that evidence of the software program and how it operates may assist his expert in explaining how law enforcement may have erroneously concluded that he was distributing such material. Owens also contends that the information requested is necessary in order for him to assess whether there was any intrusion of his personal property, in violation of the Fourth Amendment, leading to the discovery of evidence that provided the basis of the warrant utilized to search his home and computers. For these and other reasons, Owens requests that the government be directed to disclose the investigative BitTorrent software TDR, as well as related documents.

The government opposes Owens' motion on the ground that the information sought is not material to the defense and is protected under the law enforcement investigatory privilege. The law enforcement investigatory privilege is a qualified, common law privilege protecting law enforcement investigatory files from discovery. *Dellwood Farms, Inc. v. Cargill, Inc.*, 128 F.3d 1122, 1126 (7th Cir. 1997). "The purpose of this privilege is to prevent disclosure of law enforcement techniques and procedures, to preserve the confidentiality of sources, to protect witness and law enforcement personnel, to safeguard the privacy of individuals involved in an investigation, and otherwise to prevent interference with an investigation." *In re Dept. of Inv. of City of N.Y.*, 856

F.2d 481, 484 (2d Cir. 1988); *see also United States v. Winner*, 641 F.2d 825, 831 (10th Cir. 1981) ("The law enforcement investigative privilege is based primarily on the harm to law enforcement efforts which might arise from public disclosure of . . . investigatory files."). The government contends that disclosure of the information Owens seeks in this case would result in irreversible harm to pending and ongoing criminal investigations. The government further contends that the likely harm to its investigative ability far outweighs any benefit Owens might receive from disclosure of the information.

Finding itself unable to decide Owens' motion without a more complete development of the record, the court held an evidentiary hearing on the motion on August 14, 2019, at which it heard testimony from both the defense and the government technical witnesses. The parties have also submitted post hearing briefs arguing their respective positions. Having considered the evidence and arguments offered by the parties, the court concludes that the defendant's motion should be denied.

BACKGROUND

BitTorrent is a peer-to-peer (P2P) file sharing network that is used to distribute large amounts of data over the Internet, such as movies, videos, and music. "Instead of relying on a single server to provide an entire file directly to another computer, which can cause slow download speeds, BitTorrent users can download portions of the file from numerous other BitTorrent users simultaneously, resulting in faster download speeds." *United States v. Gonzales*, No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at *1 (D. Ariz. Feb. 19, 2019). BitTorrent is well known by law enforcement to be used to obtain and distribute child pornography throughout this country and the world. The court explained how the program generally works in *Gonzales*:

> To download and share files over the BitTorrent network, a user must install a BitTorrent software "client" on his computer and download a "torrent" from a torrent-search website. A torrent is a text-file containing instructions on how to find, download, and assemble the pieces of the image or video files the user wishes to view. The client software reads the instructions in the torrent, finds the pieces of the target file from other BitTorrent users who have the same torrent, and downloads and assembles the pieces, producing a complete file. The client software also makes the file accessible to the other BitTorrent users in a shared folder on the user's computer.

Id.

TDR is a modified version of the BitTorrent protocol developed by law enforcement in conjunction with the University of Massachusetts at Amherst. TDR acts as a BitTorrent user and searches the Internet for Internet protocol (IP) addresses offering torrents for known child pornography files. "When such an IP address is found, the program connects to that address and attempts to download the child pornography. The program generates detailed logs of the activity and communications between the program and the IP address. Unlike traditional BitTorrent programs, TDR is designed to download files only from a single IP address – rather than downloading pieces of files from multiple addresses – and does not share those files with other BitTorrent users." *Id.*

At the evidentiary hearing, the court heard from Detective Robert Erdely, one of the developers of the TDR program who is retired from the Pennsylvania State Police. Dkt. No. 25, Tr. at 49–123. Detective Erdely has numerous certifications in the computer related field and has worked extensively with law enforcement and universities in developing tools to investigate the exploitation of children on the Internet. Exhibit 1. TDR, which appears to be the culmination of his efforts, is used by law enforcement in over 60 countries to locate, investigate, and prosecute child predators. *Id.* Detective Erdely credibly testified that TDR is a simple program that has little

chance of malfunctioning. Any malfunction that did occur, Detective Erdely explained, would result not in a false positive, as Owens argued, but in no data at all. It would shut the program down. Tr. at 88:09–89:11.

Detective Erdely first explained in detail how the BitTorrent program works. He explained that the torrent file, which is a set of instructions for how to get the actual files they describe, is obtained by searching outside websites. The torrent is then loaded into the BitTorrent program which then sends it out to the BitTorrent network. The network then lists IP addresses that are associated with the same torrent. The different computers then engage in what Detective Erdely metaphorically described as "conversations" where "some handshaking goes on" in which they verify that they are talking about the same torrent which is identified by what is called an info hash, a lengthy digital identifier as unique as DNA. Tr. at 53:14–62:25. As Detective Erdely explained, TDR does not invade the shared space of the computer that connects to it; it only downloads what the sharing computer makes available. *Id.* at 102:17–103:13.

With TDR, law enforcement inputs torrents from its database that are known to be associated with child pornography. The torrent is loaded into the BitTorrent program and then the investigator simply waits for another member of the network to respond. Unlike the BitTorrent program, TDR connects with only a single IP address. When an IP address is found, the program connects to that address and downloads the child pornography. The program generates a detailed log of the activity and communications between the program and the IP address. In describing how TDR operated in this case, Detective Erdely highlighted the pertinent sections of the detailed logs that were generated on May 21, and again on May 22, 2018, when the downloads from Owens' computer occurred. *Id.* at 65:6–73:14; Exhibits 2 and 3. The two logs detail the download of a 226 piece file from Owens' computer on each occasion. And as for why the downloaded video was not

found on Owens' computer after it was seized by law enforcement in execution of a search warrant, Detective Erdely explained that Owens had simply deleted the file after viewing it. From his own viewing of the mirror image of Owens' computer, Detective Erdely was able to identify evidence in three different areas that the file had been on Owens' computer prior to law enforcement's execution of the search warrant. Tr. at 77:14–83:25; Exhibits 4, 5, and 6.

Finally, Detective Erdely testified that disclosure of the TDR program to defense witnesses or allowing independent testing would jeopardize ongoing and future child pornography investigations. It would expose "each and every torrent file we're investigating." Tr. at 84:13. Detective Erdely testified that it had taken eight years to build up the hash values of known child pornography files, which are key to the operation of TDR. Allowing defense witnesses access to their program exposes the files and hash values law enforcement investigates, the contact information for law enforcement and the IP addresses they are actively investigating. He compared allowing defense experts and attorneys access to "dropping a civilian in the mix of a raid." Moreover, Detective Erdely could think of no benefit a defendant would obtain from access to TDR beyond what he would know from familiarity with the BitTorrent program. *Id.* at 84:19–86:25. And since forensic analysis of Owens' computer confirmed that the same video downloaded by law enforcement was on his computer at the time, there was no need for risking such damage to this important investigative tool. *Id.* 87:1–16.

ANALYSIS

A. Materiality

Under Rule 16(a)(1)(E), the government must disclose to the defense any "books, papers, documents, data, . . . or portions of any of these items, if the item is within the government's

possession, custody, or control and: (i) the item is material to preparing the defense[.]" Fed. R. Crim. P. 16(a)(1)(E). To obtain disclosure under subsection (i) "[a] defendant must make a threshold showing of materiality[.]" *United States v. Budziak*, 697 F.3d 1105, 1111 (9th Cir. 2012) (citing *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)). To show materiality, the defendant must demonstrate that the requested evidence bears some abstract logical relationship to the issues in the case. There must be some indication that the pretrial disclosure of the disputed evidence would enable the defendant significantly to alter the quantum of proof in his favor. *United States v. Lloyd*, 992 F.2d 348, 350–51 (D.C. Cir. 1993).

In an effort to establish the materiality of the requested evidence, Owens offered the testimony of his expert, Peyton Engel. Engel is an attorney who works for a law firm in Madison, Wisconsin. In addition to his law degree, Engel has specialized in computer security for the past 16 years. His work includes conducting forensic investigations and incident response. He holds a certification as an Information Systems Security Professional and speaks at trainings and conferences, primarily for the state public defender, on how litigators should work with computer experts. He has written at least one article on cell phone forensics for a criminal defense lawyers publication and testified in state court as an expert witness on approximately ten occasions.

Engel testified that a universal truth about computer software is that there are always bugs, errors, or malfunctions in it. Tr. 7:19–23. Such a malfunction or computer error, he testified, could result in a false positive result showing that the child pornography was downloaded from Owens' computer when in fact it was not. The fact that the image that Torrential Downpour software reported had been downloaded from Owens' computer was not found on any of the media seized from his home upon execution of the software, Engel believed, was evidence of such a malfunction

or false positive. Engel testified that he needed access to the program to confirm whether Torrential Downpour actually conducts single source downloads in the way that the prosecution claims.

The mere fact that computer software can have "bugs" or errors is insufficient to show materiality under the circumstances of this case. To be "material" for purposes of Rule 16, the evidence must have "more than . . . [an] abstract logical relationship to the issues." *United States v. Ross*, 511 F.2d 757, 762 (5th Cir.) (citation omitted), *cert. denied*, 423 U.S. 836 (1975). "There must be some indication that the pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor." *Id.* at 763. The materiality requirement typically "'is not a heavy burden;' rather, evidence is material as long as there is a strong indication that . . . [the evidence] will 'play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal.'" *United States v. Lloyd*, 992 F.2d 348, 351 (D.C. Cir. 1993) (quoting *United States v. George*, 786 F. Supp. 56, 58 (D.D.C. 1992)). Under Rule 16, the defendant cannot rely on conclusory allegations or on a general description of the requested information, but must make a prima facie showing of materiality to obtain the requested information. *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990). Stated simply, the defendant must come forth with facts tending to show "that the Government is in possession of information helpful to the defense." *Id.* at 1219 (citation omitted).

Owen's effort to show materiality here falls significantly short. As Detective Erdely explained, while it may be true that complex computer programs and operating systems, like Microsoft Word with millions of lines of code, frequently have "bugs", BitTorrent is "a very, very light-weight, small protocol. A BitTorrent program like BitTorrent or uTorrent are like a couple

of megabytes." Tr. 88:18–20. The one difficulty the developers of TDR had resulted from their failure to account for the long file names exceeding 260 characters. This problem, which was promptly solved, resulted in the program shutting down, not a false positive. Detective Erdely testified that the fact that BitTorrent relies on SHA-1 hashing, which is extremely accurate, means getting a false positive is virtually impossible. Tr. 88:18–89:10. More importantly, Detective Erdely was able to point to evidence on Owens' computer showing that the child pornography files downloaded by law enforcement using TDR had been on his computer at the time of the downloads and thus must have been deleted sometime before the search warrant on his home was executed and his computer seized. It is also clear from the very nature of the BitTorrent protocol that TDR interacts with that no intrusion is made into any constitutionally protected areas as part of the initial investigation. Given these facts, Owens' expert's mere observation that complex computer software systems frequently have "bugs" is insufficient to establish materiality.

Owens contends that TDR is "effectively the key witness upon whose testimony [the government] will rely to prove its case (at least as to Count 1)." Post-Hearing Reply, Dkt. No. 28, at 1. Disclosure of the TDR source code and related information is needed, he argues, so that he can confront this witness and show possible bias. But TDR is not a witness; it is a computer program. TDR cannot testify; it will not be subject to cross-examination whether Owens' motion is granted or not. Instead, either Detective Erdely or someone else with knowledge of how it works will testify, and Owens will be free to cross-examine that witness. On this record, Owens has failed to show how knowledge of the TDR program or related information will assist his defense. BitTorrent is the program by which he allegedly distributed child pornography, and the government

has placed no limitation on his ability to fully investigate the internal workings and operation of that program.

Just as the defendant did in *United States v. Maurek*, "[i]n conclusory fashion, [Owens] states the information 'is necessary to aid the suppression motion, to permit [him] to confront evidence against him, and to establish a defense through independent expert analysis of this software." No. CR-15-129-D, 2015 WL 12915605, at *3 (W.D. Okla. Aug. 31, 2015). As in that case, however, Owens "fails to present this Court with any specific facts which would tend to show how production and/or inspection of the 'Torrential Downpour' software would enable him to significantly 'alter the quantum of proof in his favor.'" *Id.* (quoting *United States v. King*, 928 F. Supp. 1059, 1061–62 (K. Kan. 1996)). He has therefore failed to establish that the evidence he seeks is material to his defense.

B. Law Enforcement Investigatory Privilege

The party asserting the law enforcement privilege has the burden to establish the privilege applies to the documents or information in question. *In re The City of N.Y.*, 607 F.3d 923, 944, 948 (2nd Cir. 2010). "To meet this burden, the party asserting the law enforcement privilege must show that the documents contain information that the law enforcement privilege is intended to protect." *Id.* This would include "information pertaining to 'law enforcement techniques and procedures,' information that would undermine 'the confidentiality of sources,' information that would endanger 'witness and law enforcement personnel [or] the privacy of individuals involved in an investigation,' and information that would 'otherwise . . . interfere[ ] with an investigation.'" *Id.* (quoting *In re Dep't of Investigation of City of N.Y.*, 856 F.2d 481, 484 (2d Cir. 1988)). It would also include information disclosure of which "would hamper future law enforcement efforts by

enabling adversaries of law enforcement to evade detection." *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 1002 (D. Ariz. 2012). After a litigant shows the privilege applies, a court engages in a balancing process to decide whether the litigant's need for access to the privileged information outweighs the public's interest in nondisclosure. *Id.* at 948. As the Eighth Circuit stated when addressing a state court's refusal to disclose the identity of a confidential informant in the context of a state habeas proceeding, "the decision to order disclosure varies with the particular circumstances of each case." *Barnes v. Dormire*, 251 F.3d 767, 770 (8th Cir. 2001) (citing *Roviaro v. United States*, 353 U.S. 53, 62 (1957)). Ultimately, the test is one of necessity: "Where the disclosure of [the requested information] . . . is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause, the privilege must give way." *Roviaro*, 353 U.S. at 60–61.

Based on the evidence presented at the hearing, the court finds that the law enforcement investigatory privilege extends to TDR. Detective Erdely testified that providing access to TDR to Owens' expert would risk disclosure of thousands of torrents and hash values it has taken law enforcement years to amass. Although as a general matter, some individual hash values or torrents are publicly available, what the public doesn't know is what areas law enforcement is active in and which hash values and torrents it is using. According to Detective Erdely, "to put that out there would give them the key to not get caught." Tr. 114:17–18. Detective Erdely acknowledged that a person could promise never to disclose the information, but noted that such promises are not always kept and that once the information was disclosed, law enforcement would have to start from scratch to rebuild its database. Tr. 84:14–25. Given this risk and the failure to show the materiality of the information sought to the defense, the court concludes that Owens' motion to compel should be denied.

The courts reached the same conclusion when confronted with similar facts in *United States v. Feldman*, No. 13-CR-155, 2014 WL 7653617 (E.D. Wis. July 7, 2014), and *United States v. Hoeffener*, No. 4:16CR00374, 2017 WL 3676141 (E.D. Mo. Aug 25, 2017). It is true that the defendants in both *Feldman* and *Hoeffener*, were not charged with distribution of child pornography based on downloads to the Torrential Downpour program. As a result, the charges in those cases were not related to conduct that occurred over the peer-to-peer network. Still, both courts rejected the defendants' arguments that disclosure of the Torrential Downpour program and related materials was necessary for counsel to investigate a possible Fourth Amendment violation. As in this case, there was no evidence presented that the files downloaded in those cases were obtained by Torrential Downpour accessing non-public parts of the defendants' computers. And while the distribution charge in this case does rely on evidence obtained during the TDR download, Erdely's testimony concerning how the program operates and the fact that evidence of the same files was found on Owens' computer, thereby confirming that he possessed the video at the time of the download, have not been challenged.

In light of this evidence, and absent any showing by the defense as to how the requested information is material, Owens' motion to compel must be denied. Whatever relevance the evidence sought may have to the case is substantially outweighed by the risk that it would be disclosed and thereby allow those willing and able to circumvent law enforcement's investigatory tools to develop methods of sharing child pornography that would go undetected.

CONCLUSION

For the reasons set forth above, the court finds that Owens has failed to establish that the information sought in his discovery request is material to his defense. The court also finds that the

information requested is protected by the law enforcement investigatory privilege and that the public interest in non-disclosure substantially outweighs any interest of the defendant in acquiring it. Owens has failed to show that disclosure of further information related to TDR is either relevant or helpful to the defense.

SO ORDERED at Green Bay, Wisconsin this 18th day of December, 2019.

s/ William C. Griesbach
William C. Griesbach, District Judge
United States District Court